Substitute for Form 1449 A & B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	1	of	1

Complete if known

Application Number	Not Yet Assigned
Confirmation Number	Not Yet Assigned
Filing Date	December 19, 2005
First Named Inventor	Isamu TERANISI
Art Unit	Not Yet Assigned
Examiner Name	Not Yet Assigned
Attorney Docket Number	Q92077

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number: Number	Document Number: Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
O.A.		US 6,081,597	A	06-27-2000	NTRU Cryptosystems, Inc.
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document: Country Code[3]	Foreign Patent Document: Number[4]	Foreign Patent Document: Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Translation[6]
O.A.		JP	2000-516733	A	12-12-2000		
O.A.		WO	98/08323	A1	02-26-1998		
O.A.		AU	4582897	A	03-06-1998		
O.A.		CA	2 263 588	A	01-18-2005		
O.A.		CN	1232588	A	10-20-1999		

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city, and/or country where published.	Translation[6]
O.A.		Victor Shoup, "OAEP RECONSIDERED (Extended Abstract)," LNCS, Vol. 2139, 2001, pages 239 to 259.	
O.A.		Phong Q. Nguyen, et al. "ANALYSIS AND IMPROVEMENTS OF NTRU ENCRYPTION PADDINGS," LNCS, Vol. 2442, 2002, pages 210 to 225.	
O.A.		John A. Proos, "IMPERFECT DECRYPTION AND AN ATTACK ON THE NTRU ENCRYPTION SCHEME," University of Waterloo, January 7, 2003, pages 1 to 28.	
O.A.		Eliane Jaulmes, et al. "A CHOSEN-CIPHERTEXT ATTACK AGAINST NTRU," Crypto 2000 Springer Lecture Notes in Computer Sciences, 2000, pages 20 to 35.	
O.A.		Jeffrey Hoffstein, et al. "PROTECTING NTRU AGAINST CHOSEN CIPHERTEXT AND REACTION ATTACKS," NTRU Cryptosystems Technical Report, Report #016, Version 1, June 9, 2000, pages 1 to 6.	
O.A.		Jeffrey Hoffstein, et al. "OPTIMIZATIONS FOR NTRU," NTRU Cryptosystems, Inc., pages 1 to 12.	
O.A.		Joseph H. Silverman, "PLAINTEXT AWARENESS AND THE NTRU PKCS," NTRU Cryptosystems Technical Report, Report #007, Version 2, June 2000, pages 1 to 7.	
O.A.		Don Coppersmith, et al. "LATTICE ATTACKS ON NTRU," Eurocrypt '97 Springer Lecture Notes in Computer Sciences, 1997, pages 52 to 61.	
O.A.		Jeffrey Hoffstein, et al. "NTRU: A RING-BASED PUBLIC KEY CRYPTOSYSTEM".	

Examiner Signature	Daniel O. Owen	Date Considered	4/11/07

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]See Kind Codes of USPTO Patent Documents at www.uspto.gov, MPEP 901.04 or in the comment box of this document. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST. 3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to indicate here if English language Translation is attached.